THE CLAIMS

What is claimed is:

1. A method for creating a virtual private network (VPN) over a telecommunications network, comprising steps of:

sending a request from a first VPN device to a second VPN device for establishing a VPN between the first and second VPN devices, the request including a first signed certificate having at least one verified VPN parameter for the first VPN device; and

receiving a reply at the first VPN device from the second VPN device, the reply including a second signed certificate having at least one verified VPN parameter for the second VPN device; and

establishing the VPN between the first and second VPN devices based on each verified VPN parameter for each of the first and second VPN devices.

2. The method according to claim 1, further comprising a step of sending a request from the first VPN device to an on-line database connected to the telecommunications network for obtaining a secure domain name address associated with the second VPN device.

3. The method according to claim 2, wherein the step of sending the request from the first VPN device to the second VPN device sends the request to the secure domain

name address associated with the second VPN device.

4. The method according to claim 1, wherein the step of sending the request from the first VPN device to the second VPN device for establishing the VPN further includes receiving a request for establishing the VPN from a client device that is associated with the first VPN.

5. The method according to claim 4, wherein the request received from the client device includes a destination designation for the VPN.

6. The method according to claim 4, wherein the request received from the client device includes a source/destination designation for the VPN.

7. The method according to claim 6, wherein the source/destination designation includes a wild card designation.

8. The method according to claim 1, further comprising a step of verifying at the first VPN device the second signed certificate having at least one verified VPN parameter for the second VPN device.

9. The method according to claim 8, wherein the step of verifying the second signed certificate includes a step of sending a request from the first VPN device to an on-line database for obtaining a public key associated with the second VPN device.

10. The method according to claim 9, further comprising a step of verifying at the second VPN device the first signed certificate having at least one verified VPN parameter for the first VPN device.

11. The method according to claim 10, wherein the step of verifying the first signed certificate includes a step of sending a request to an on-line database from the second VPN device for obtaining a public key associated with the first VPN device.

12. The method according to claim 1, further comprising steps of:

determining at the second VPN device whether a policy rule prevents a VPN connection to the first VPN device; and

sending the reply to the first VPN device from the second VPN device when no policy rule prevents a VPN connection to the first VPN device, and not sending the reply to the first VPN when a policy rule prevents a VPN connection to the first VPN device.

13. The method according to claim 1, wherein the telecommunications network is

the Internet.

14. The method according to claim 1, wherein the step of establishing the VPN between the first and second VPN devices establishes a standing VPN connection.

15. The method according to claim 1, wherein the step of establishing the VPN between the first and second VPN devices establishes a VPN of opportunity.

16. A method for creating a virtual private network (VPN) over a telecommunications network, comprising steps of:

receiving a request from a first VPN device at a second VPN device for establishing a VPN between the first and second VPN devices, the request including a first signed certificate having at least one verified VPN parameter for the first VPN device; and

sending a reply to the first VPN device from the second VPN device, the reply including a second signed certificate having at least one verified VPN parameter for the second VPN device; and

establishing the VPN between the first and second VPN devices based on each verified VPN parameter for each of the first and second VPN devices.

17. The method according to claim 16, further comprising a step of sending a

request from the second VPN device to an on-line database connected to the telecommunications network for obtaining a secure domain name address associated with the second VPN device.

18. The method according to claim 16, further comprising a step of verifying at the second VPN device the first signed certificate having at least one verified VPN parameter for the first VPN device.

19. The method according to claim 18, wherein the step of verifying the first signed certificate includes a step of sending a request from the second VPN device to an on-line database for obtaining a public key associated with the first VPN device.

20. The method according to claim 16, further comprising steps of:

determining at the second VPN device whether a policy rule prevents a VPN connection to the first VPN device; and

sending the reply to the first VPN device from the second VPN device when no policy rule prevents a VPN connection to the first VPN device, and not sending the reply to the first VPN when a policy rule prevents a VPN connection to the first VPN device.

21. The method according to claim 16, wherein the telecommunications network

is the Internet.

22. The method according to claim 16, wherein the step of establishing the VPN between the first and second VPN devices establishes a standing VPN connection.

23. The method according to claim 16, wherein the step of establishing the VPN between the first and second VPN devices establishes a VPN of opportunity.

24. A method for creating a virtual private network (VPN) over a telecommunications network, comprising steps of:

sending a certificate request for a virtual private network (VPN) device to a certification authority connected to the telecommunications network, the certificate request including at least one VPN parameter that will be used by the VPN device for establishing a VPN over the telecommunications network;

receiving a signed certification from the certification authority, the signed certification containing the at least one VPN parameter contained in the certificate request; and

configuring the VPN device to operate in accordance with the at least one VPN parameter contained in the signed certificate.

25. The method according to claim 24, wherein the certificate request includes at least one telecommunications network address that the VPN device will use as a client network address for a VPN established through the VPN device.

26. The method according to claim 25, wherein the certificate request includes a range of telecommunications network addresses that the VPN device will use as client network addresses for VPNs established through the VPN device.

27. The method according to claim 24, further comprising steps of:

exchanging the signed certificate with another VPN device at a selected telecommunications network address; and

establishing a VPN in accordance with the at least one VPN parameter contained in the signed certificate.

28. The method according to claim 27, wherein the step of establishing the VPN is further based on a source and destination name pair.

29. The method according to claim 28, wherein the source and destination name pair includes a wild card designation.

30. The method according to claim 27, wherein the step of establishing the VPN is further based on at least one rule allowing a VPN connection to the selected telecommunications network address.

31. The method according to claim 27, wherein the step of establishing the VPN is further based on a Quality of Service parameter.

32. The method according to claim 27, wherein the step of establishing the VPN is further based on a bandwidth limitation parameter.

33. The method according to claim 24, wherein the telecommunications network is the Internet.

34. The method according to claim 24, further comprising steps of:

receiving a request from a client device connected to the VPN device for establishing a VPN connection to a selected telecommunications network address; and

querying an on-line database connected to the telecommunications network for obtaining a secure domain name address for the selected telecommunications network address,

wherein the step of establishing the VPN connection to the selected

telecommunications network address is performed when the on-line database contains the secure domain name address for the selected telecommunications network address.

35. The method according to claim 34, wherein the request for establishing the VPN contains a source and destination name pair.

36. The method according to claim 24, further comprising a step of sending at least one VPN parameter for the VPN device that is not contained in the certificate request to the certification authority for verification by the certificate authority.

37. The method according to claim 24, further comprising steps of:

receiving the certificate request for the VPN device from the VPN device at the certification authority;

verifying at the certification authority the at least one VPN parameter contained in the certificate request; and

sending the signed certification to the VPN device when each VPN parameter contained in the certificate request is verified.

38. The method according to claim 37, wherein the certificate request includes at least one telecommunications network address that the VPN device will use as a client

network address for a VPN established through the VPN device,

wherein the step of verifying verifies each telecommunication network address contained in the certificate request.

39. The method according to claim 37, wherein the certificate request includes a range of telecommunications network addresses that the VPN device will use as client network addresses for VPNs established through the VPN device,

wherein the step of verifying verifies the range of telecommunications network addresses contained in the certificate request.

40. The method according to claim 24, further comprising steps of:

receiving a request at an on-line database connected to the telecommunications network from the VPN device for a secure domain name address for a selected VPN device connected to the telecommunications network; and

sending the secure domain name address for the selected VPN device to the requesting VPN device when the secure domain name address for the selected VPN device is contained in the online database.

41. The method according to claim 24, further comprising steps of:

receiving at the certification authority at least one VPN parameter for the VPN

device that is not contained in the certificate request; and

storing the at least one received VPN parameter that is not contained in the certificate request in an on-line database.

42. A method for creating a virtual private network (VPN) over a telecommunications network, comprising steps of:

receiving at a certification authority a certificate request for a VPN device connected to the telecommunications network, the certificate request including at least one VPN parameter that will be used for establishing a VPN over the telecommunications network;

verifying at the certification authority each VPN parameter contained in the certificate request; and

sending a signed certification to the VPN device when each VPN parameter contained in the certificate request is verified.

43. The method according to claim 42, wherein the certificate request includes at least one telecommunications network address that the VPN device will use for establishing a VPN, and

wherein the step of verifying verifies each telecommunication network address contained in the certificate request.

44. The method according to claim 43, wherein the certificate request includes a range of telecommunications network addresses that the VPN device will use for VPNs established through the VPN device, and

wherein the step of verifying verifies the range of telecommunications network addresses contained in the certificate request.

45. The method according to claim 43, wherein the telecommunications network is the Internet.

46. A virtual private network (VPN) device, comprising:

a memory containing a certificate that has been signed by a certification authority, the signed certificate containing at least one VPN parameter for the VPN device that has been verified by the certification authority; and

a processor receiving a request for establishing a VPN and responds to the request by sending the signed certificate over a telecommunications network to a second VPN device based on the received request.

47. The VPN device according to claim 46, wherein the request is received from the second VPN device, and a signed certificate for the second VPN device, the

signed certificate for the second VPN device containing at least one VPN parameter for the second VPN device that has been verified by a certification authority.

48. The VPN device according to claim 47, wherein the processor verifies the signed certificate for the second VPN device before sending the signed certificate to the second VPN device.

49. The VPN device according to claim 48, wherein the processor verifies the signed certificate for the second VPN device using a public key associated with the second VPN device.

50. The VPN device according to claim 47, wherein the processor establishes a VPN based on each verified VPN parameter for the VPN device and based each verified VPN parameter for the second VPN device.

51. The VPN device according to claim 46, wherein the request is received from a client device associated with the VPN device,

wherein the processor sends a request to an on-line database connected to the telecommunications network for obtaining a secure domain name address associated with the second VPN device, and

wherein the processor sends the signed certificate over the telecommunications network to the secure domain name address associated with the second VPN device.

52. The VPN device according to claim 51, wherein the request received from the client device includes a destination designation for the VPN.

53. The VPN device according to claim 51, wherein the request received from the client device includes a source/destination designation for the VPN.

54. The VPN device according to claim 51, wherein the source/destination designation includes a wild card designation.

55. The VPN device according to claim 46, wherein the processor determines whether a policy rule contained in the memory prevents a VPN connection to the second VPN device; and

wherein the processor sends the certificate to the second VPN device when no policy rule contained in the memory prevents a VPN connection to the second VPN device.

56. The VPN device according to claim 46, wherein the telecommunications

network is the Internet.

57. The VPN device according to claim 46, wherein the request for establishing a VPN is a request for establishing a standing VPN connection.

58. The VPN device according to claim 46, wherein the request for establishing a VPN is a request for establishing a VPN of opportunity.

59. The VPN device according to claim 46, wherein the VPN device is one of a VPN concentrator, a router, a firewall and a host computer.

60. A computer-readable medium containing computer executable instructions for performing steps of:

sending a request from a first VPN device to a second VPN device for establishing a VPN between the first and second VPN devices, the request including a first signed certificate having at least one verified VPN parameter for the first VPN device; and

receiving a reply at the first VPN device from the second VPN device, the reply including a second signed certificate having at least one verified VPN parameter for the second VPN device; and

establishing the VPN between the first and second VPN devices based each

verified VPN parameter for each of the first and second VPN devices.

61. The computer-readable medium according to claim 60, further comprising a step of sending a request from the first VPN device to an on-line database connected to the telecommunications network for a secure domain name address associated with the second VPN device.

62. The computer-readable medium according to claim 61, wherein the step of sending the request from the first VPN device to the second VPN device sends the request to the secure domain name address associated with the second VPN device.

63. The computer-readable medium according to claim 60, wherein the step of sending the request from the first VPN device to the second VPN device for establishing the VPN further includes receiving a request for establishing the VPN from a client device that is associated with the first VPN.

64. The computer-readable medium according to claim 63, wherein the request received from the client device includes a destination designation for the VPN.

65. The computer-readable medium according to claim 63, wherein the request

received from the client device includes a source/destination designation for the VPN.

66. The computer-readable medium according to claim 65, wherein the source/and destination designation includes a wild card designation.

67. The computer-readable medium according to claim 60, further comprising a step of verifying at the first VPN device the second signed certificate having at least one verified VPN parameter for the second VPN device.

68. The computer-readable medium according to claim 67, wherein the step of verifying the second signed certificate includes a step of sending a request from the first VPN device to an on-line database for a public key associated with the second VPN device.

69. The computer-readable medium according to claim 68, further comprising a step of verifying at the second VPN device the first signed certificate having at least one verified VPN parameter for the first VPN device.

70. The computer-readable medium according to claim 69, wherein the step of verifying the first signed certificate includes a step of sending a request to an on-line database from the second VPN device for a public key associated with the first VPN device.

71. The computer-readable medium according to claim 60, further comprising steps of:

determining at the second VPN device whether a policy rule prevents a VPN connection to the first VPN device; and

sending the reply to the first VPN device from the second VPN device when no policy rule prevents a VPN connection to the first VPN device, and not sending the reply to the first VPN when a policy rule prevents a VPN connection to the first VPN device.

72. The computer-readable medium according to claim 60, wherein the telecommunications network is the Internet.

73. The computer-readable medium according to claim 60, wherein the step of establishing the VPN between the first and second VPN devices establishes a standing VPN connection.

74. The computer-readable medium according to claim 60, wherein the step of establishing the VPN between the first and second VPN devices establishes a VPN of opportunity.

75. A computer-readable medium containing computer-executable instructions for performing steps of:

sending a certificate request for a virtual private network device to a certification authority connected to the telecommunications network, the certificate request including at least one VPN parameter that will be used by the VPN device for establishing a VPN over the telecommunications network;

receiving a signed certification from the certification authority, the signed certification containing the at least one VPN parameter contained in the certificate request; and

configuring the VPN device to operate in accordance with the at least one VPN parameter contained in the signed certificate.

76. The computer-readable medium according to claim 75, wherein the certificate request includes at least one telecommunications network address that the VPN device will use as a client network address for a VPN established through the VPN device.

77. The computer-readable medium according to claim 75, wherein the certificate request includes a range of telecommunications network addresses that the VPN device will use as client network addresses for VPNs established through the VPN device.

78. The computer-readable medium according to claim 75, wherein the telecommunications network is the Internet.

79. A computer-readable medium containing computer-readable instructions for performing steps of:

receiving at a certification authority a certificate request for a VPN device connected to the telecommunications network, the certificate request including at least one VPN parameter that will be used for establishing a VPN over the telecommunications network;

verifying at the certification authority each VPN parameter contained in the certificate request; and

sending a signed certification to the VPN device when each VPN parameter contained in the certificate request is verified.

80. The computer-readable medium according to claim 79, wherein the certificate request includes at least one telecommunications network address that the VPN device will use for establishing a VPN, and

wherein the step of verifying verifies each telecommunication network address contained in the certificate request.

81. The computer-readable medium according to claim 80, wherein the certificate request includes a range of telecommunications network addresses that the VPN device will use for VPNs established through the VPN device, and

wherein the step of verifying verifies the range of telecommunications network addresses contained in the certificate request.

82. The computer-readable medium according to claim 79, wherein the telecommunications network is the Internet.